Gérer les identités R 56

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * identifier le personnel et les systèmes de façon unique * permettre une attribution appropriée des droits d’accès |
| pilote | responsable sécurité de l’information |
| risques | * ne pas protéger les identifiants attribués * ne pas préserver les identifiants * ne pas gérer les incidents * ne pas évaluer les risques liés aux identifiants * ne pas prendre en compte les risques identifiés * ne pas gérer les comptes dormants |
| processus amont | * planifier le SMSI * apprécier les risques * traiter les risques * utiliser la cryptographie * enregistrer et désinscrire * appliquer la sécurité de l’information * communiquer |
| processus aval | * gérer l’authentification * gérer la chaîne TIC * gérer les incidents * gérer les changements * supprimer l’information * distribuer les accès |
| éléments d'entrée | * risques identifiés * liste du personnel et des systèmes |
| activités  (sous-processus) | * attribuer à chaque personne ou système un identifiant unique * attribuer des identifiants partagés seulement pour des cas exceptionnels (validation spéciale) * attribuer des identifiants d’entités non humaines avec validation spéciale * supprimer les identifiants qui ne sont plus nécessaires * gérer les incidents * conserver les enregistrements de tous les identifiants * gérer les accès à l’information et aux autres actifs |
| éléments de sortie | * inventaire des identifiants * enregistrement et désinscription |
| ressources | moyens techniques et informatiques |
| indicateurs | * taux d’identités renouvelées * taux d’incidents |
| procédures / documents | incidents, continuité d’activité, sensibilisation et formation, restrictions d’accès, gestion des vulnérabilités / enregistrement et désinscription, inventaire, registre des incidents, vulnérabilités techniques, engagement de confidentialité |
| clients | l’ensemble du personnel |

Glossaire :

SMSI : système de management de la sécurité de l’information

TIC : technologie de l’information et de la communication

responsable sécurité de l’information

* identifier le personnel et les systèmes de façon unique
* permettre une attribution appropriée des droits d’accès

gérer les identités / R 56

risques

processus amont

processus aval

* gérer l’authentification
* gérer la chaîne TIC
* gérer les incidents
* gérer les changements
* supprimer l’information
* distribuer les accès
* ne pas protéger les identifiants attribués
* ne pas préserver les identifiants
* ne pas gérer les incidents
* ne pas évaluer les risques liés aux identifiants
* ne pas prendre en compte les risques identifiés
* ne pas gérer les comptes dormants
* planifier le SMSI
* apprécier les risques
* traiter les risques
* utiliser la cryptographie
* enregistrer et désinscrire
* appliquer la sécurité de l’information
* communiquer

activités

éléments d'entrée

éléments de sortie

* attribuer à chaque personne ou système un identifiant unique
* attribuer des identifiants partagés seulement pour des cas exceptionnels (validation spéciale)
* attribuer des identifiants d’entités non humaines avec validation spéciale
* supprimer les identifiants qui ne sont plus nécessaires
* gérer les incidents
* conserver les enregistrements de tous les identifiants
* gérer les accès à l’information et aux autres actifs
* inventaire des identifiants
* enregistrement et désinscription
* risques identifiés
* liste du personnel et des systèmes

ressources

indicateurs

clients

procédures / documents

incidents, continuité d’activité, sensibilisation et formation, restrictions d’accès, gestion des vulnérabilités / enregistrement et désinscription, inventaire, registre des incidents, vulnérabilités techniques, engagement de confidentialité

taux d’identités renouvelées, taux d’incidents

l’ensemble du personnel

moyens techniques et informatiques